The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/14/2020

SUBJECT:
A Vulnerability in IBM WebSphere Application Server Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in IBM WebSphere Application Server that could allow for remote code execution. IBM WebSphere Application Server is a software framework and middleware that hosts Java-based web applications. Successful exploitation of this vulnerability could allow an attacker to execute remote code in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

THREAT INTELLIGENCE:
There are no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- IBM Websphere Application Server version 8.5.0.0 through 8.5.5.18
- IBM Websphere Application Server version 9.0.0.0 through 9.0.5.5
- IBM WebSphere Virtual Enterprise Edition version 7.0 through 7.0.0.45
- IBM WebSphere Virtual Enterprise Edition version 8.0 through 8.0.0.15

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in IBM WebSphere Application Server that could allow for remote code execution. The specific flaw exists only if “undocumented customization” has been

applied by an administrator. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.

Successful exploitation of this vulnerability could allow an attacker to execute remote code in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to the latest version of IBM WebSphere Application Server immediately, after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4589

IBM:
https://www.ibm.com/support/pages/security-bulletin-websphere-application-server-vulnerable-remote-code-execution-vulnerability-cve-2020-4589